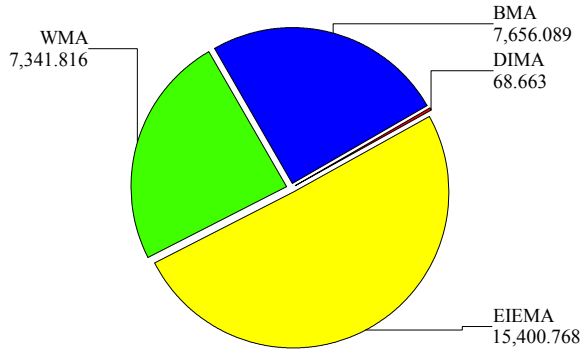
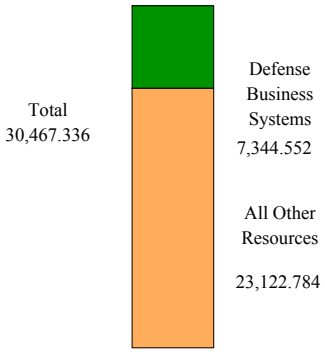
Department of Defense
Fiscal Year (FY) 2016 IT President's Budget Request
Overview

Mission Area



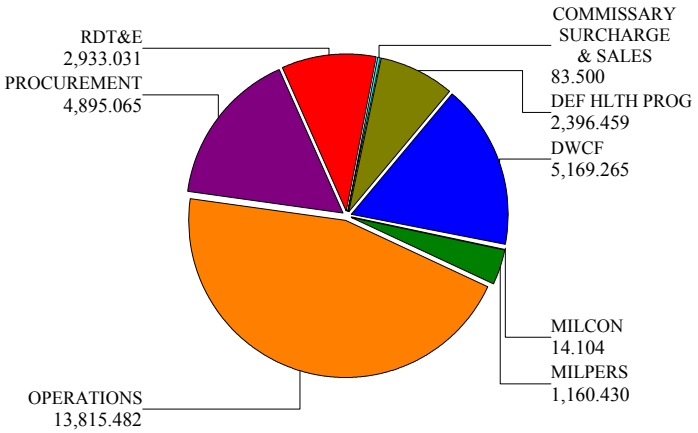
FY2016 ($M)

Business System Breakout



FY2016 ($M)

Appropriation



FY2016 ($M)

FY15 to FY16 Comparison ($M)

	FY2015	Inflation	Program Change	FY2016
PB FY2016:	29,992.051	509.862	475.285	30,467.336

Explanation:

The respective explanations for horizontal and vertical changes between and within President Budget Requests are best provided by referencing the proceeding explanations provided by each of Services, Components, and Agencies within this document.

FY15/FY16PB Comparison ($M)

	FY2015	FY2016	Delta
PB FY2015:	30,292.191	31,162.065	869.874
PB FY2016:	29,992.051	30,467.336	
Delta:	-300.140	-694.729	

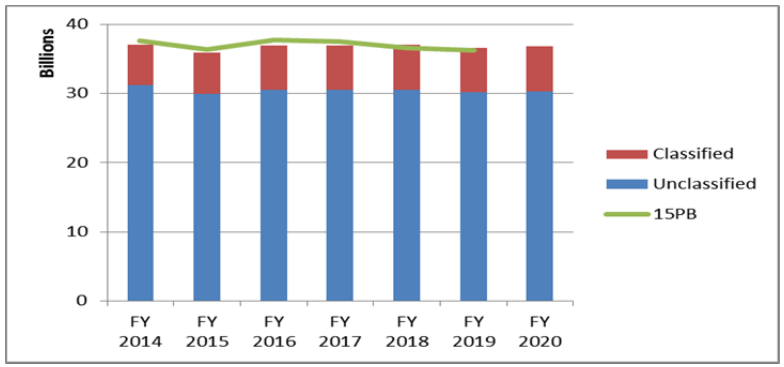
Explanation:

The respective explanations for horizontal and vertical changes between and within President Budget Requests are best provided by referencing the proceeding explanations provided by each of Services, Components, and Agencies within this document.

Page left intentionally blank

Department of Defense (DoD) Chief Information Officer (CIO)

The Department of Defense (DoD) FY2016 total Information Technology (IT) Budget Request is $36.93B and represents a $1.01B (2.8%) increase from the FY2015 enacted. This request includes both unclassified ($30.47B) and classified ($6.46B) investments. Consistent with administration guidance, the DoD IT Budget remains constant throughout the FY2016 - FY2020 Future Year Defense Plan (FYDP); factoring the future value of money DoD projects approximately $6B in decreased IT spending by FY2020. The DoD's classified IT budget request includes cyberspace operations investments and other classified IT investments; the classified IT budget is projected to remain relatively constant over the FYDP.



The DoD's networks are a mission critical resource that underpins Information Operations, Command and Control, logistics, finance, transportation, medical, maintenance and other activities. The Department's evolving infrastructure modernization efforts as envisioned in the Joint Information Environment (JIE) represents one of the critical elements. The DoD CIO is leading the implementation of the JIE with a collaborative team of experts from DoD CIO, the Joint Staff, the Services, the Defense Information Systems Agency (DISA), US Cyber Command (USCC), and other DoD agencies in planning, synchronizing, and implementing actions to enable the Department to achieve JIE. The JIE initiative proposes to increase the operational effectiveness of the DoD IT infrastructure by consolidating the Military Services' data centers and Network Operations centers and by replacing Service-specific IT security implementations with a single DoD security architecture. Implementing these initiatives will: improve the operational effectiveness of the IT infrastructure in supporting the DoD's mission; will optimize the operation of the DoD IT infrastructure; improve the security of that infrastructure; and improve access to information.

Additionally, the United States and its international partners face a world of complex national security challenges. Nowhere is this more apparent than in cyberspace. Cyberspace has emerged as a critical operational element in the military environment and ensuring the availability and dominance of cyberspace is a major challenge facing the DoD. The DoD's Cyberspace Operations and Information Assurance budget is a collection of efforts intended to operate, defend, and secure the information networks. A copy of this FY2016 classified IT annex can be obtained by contacting the office of the DoD Chief Information Officer.

(dollars in thousands)

	FY 2014	FY 2015	FY 2016	FY 2017	FY 2018	FY 2019	FY 2020
ARMY							
Unclassified	$ 8,605,265	$ 7,838,124	$ 8,061,001	$ 8,077,284	$ 8,450,508	$ 8,433,048	$ 8,140,679
Classified	$ 687,304	$ 729,381	$ 1,086,333	$ 1,078,945	$ 1,111,158	$ 1,145,475	$ 1,131,828
Subtotal	$ 9,292,569	$ 8,567,505	$ 9,147,334	$ 9,156,229	$ 9,561,666	$ 9,578,523	$ 9,272,507
Navy							
Unclassified	$ 7,007,599	$ 6,690,821	$ 6,921,037	$ 6,762,852	$ 6,649,870	$ 6,848,967	$ 6,728,662
Classified	$ 809,473	$ 810,765	$ 907,793	$ 885,979	$ 898,655	$ 888,140	$ 903,823
Subtotal	$ 7,817,072	$ 7,501,586	$ 7,828,830	$ 7,648,831	$ 7,548,525	$ 7,737,107	$ 7,632,485
Air Force							
Unclassified	$ 6,421,626	$ 6,015,825	$ 5,916,364	$ 6,388,956	$ 5,800,059	$ 5,051,776	$ 5,414,650
Classified	$ 1,336,392	$ 1,516,429	$ 1,639,355	$ 1,663,138	$ 1,670,862	$ 1,573,670	$ 1,586,322
Subtotal	$ 7,758,018	$ 7,532,254	$ 7,555,719	$ 8,052,094	$ 7,470,921	$ 6,625,446	$ 7,000,972
Defense Wide							
Unclassified	$ 9,167,260	$ 9,447,281	$ 9,568,934	$ 9,290,166	$ 9,640,077	$ 9,862,565	$ 10,022,706
Classified	$ 2,984,252	$ 2,868,807	$ 2,831,235	$ 2,759,272	$ 2,799,985	$ 2,818,557	$ 2,829,682
Subtotal	$ 12,151,512	$ 12,316,088	$ 12,400,169	$ 12,049,438	$ 12,440,062	$ 12,681,122	$ 12,852,388
Total							
Unclassified	$ 31,201,750	$ 29,992,051	$ 30,467,336	$ 30,519,258	$ 30,540,514	$ 30,196,356	$ 30,306,697
Classified	$ 5,817,421	$ 5,925,382	$ 6,464,716	$ 6,387,334	$ 6,480,660	$ 6,425,842	$ 6,451,655
Total	$ 37,019,171	$ 35,917,433	$ 36,932,052	$ 36,906,592	$ 37,021,174	$ 36,622,198	$ 36,758,352

Department of Defense Information Technology Budget Overview

The DoD CIO serves as the advisor to the Secretary of Defense and Deputy Secretary of Defense for information technology (IT) (including national security systems and defense business systems), information resources management (IRM) and efficiencies. The DoD CIO is responsible for all matters relating to the DoD information enterprise, including communications; spectrum management; network policy and standards; information systems; cybersecurity; positioning, navigation, and timing (PNT) policy; and the DoD information enterprise that supports DoD command and control (C2). As the DoD Chief Information Officer, the DoD CIO provides the leadership and guidance to implement the JIE and ultimately deliver the critical enabling capabilities required by the National Defense Strategy. Transforming the DoD Information Enterprise requires fundamental changes in process, policy and culture across the Department. The technology change will be significant, but the associated organizational change and cultural shift may be even more challenging. Timely and dependable information will be available across the enterprise: from higher level headquarters and command centers, to a soldier tracking insurgents, or a civilian in need of a new supplier. Ultimately, the role of the DoD CIO is to lead the Department to achieve an information advantage for the warfighter and our mission partners.

The DoD's IT budget is designed to deliver the DoD Information Enterprise envisioned by the National Defense Strategy, the National Military Strategy, the Quadrennial Defense Review (QDR), the Department's Strategic Management Plan (SMP) and the JIE.

The DoD Information Enterprise (IE) —which enables a new, net-centric way of working—is constructed from the information itself, as well as a set of standards, services and procedures as described in the DoD Information Enterprise Architecture, that enable information to be widely available to authorized users. The delivered set of services and tools will provide information and capabilities that enable end-user communities to more effectively and efficiently support mission operations. The IT environment investments operate in over 6,000 locations worldwide, supporting the unique needs and missions of the three Military Departments and over 40 Defense Agencies and Field Activities within the Department. Finally, the DoD Information Enterprise includes the networks over which information travels and the security protocols that protect it.

The DoD Information Resources Management Strategic Plan (IRM SP) establishes goals, objectives, and strategy elements that will move the Department toward the desired end state of the JIE, guiding the transformation of the DoD from a stove-piped information approach to achieving the Department's information sharing vision. The IRM Strategic Plan fosters alignment of the Department's information sharing efforts, particularly those specified in the JIE Implementation Plan, by identifying and relating the development and implementation of specific policies, programs, and initiatives.

The DoD CIO supports accomplishment of the goals of the IRM Strategic Plan by:

- Working with key stakeholders across the Department to ensure that information is visible, accessible, and understandable to all authorized users in a trusted environment without regard to location or time.

- Leading specific information resource capabilities including command and control, communications, IT infrastructure, and information assurance (IA), ensuring that these capabilities are architected, engineered, and delivered in a manner that optimizes the Department's mission capabilities, increases the Department's security posture, and makes most effective use of the Department's financial resources.

- Leading DoD's network cybersecurity/information assurance efforts and managing DoD enterprise information sharing risks, while at the same time protecting our information assets.

- Providing guidance and oversight with regard to overall operation and defense of the DoD Information Enterprise.

The success of DoD's information sharing environment is predicated upon achieving secure information sharing within the context of a highly contested information environment. To maximize the potential of the information sharing enterprise, solutions must enable both sharing information widely and stringent protection mechanisms.

Joint Information Environment (JIE)

The JIE is a single, secure, reliable Department of Defense (DoD)-wide information environment, comprised of shared IT infrastructure, shared data, enterprise services, and a single security architecture to achieve full spectrum superiority, improve mission effectiveness, increase security, and realize IT efficiencies.

Mission success depends upon the ability of our military commanders and civilian leaders to act decisively based on the most timely and accurate data and information. In recognition of the challenges posed by capable adversaries actively seeking to penetrate DoD systems, compromise command and control, and steal or destroy sensitive and strategic information, DoD is undertaking an ambitious effort to re-align and restructure how DoD's many IT networks are constructed, operated, resourced, and defended. The alignment and modernization of the Department's existing vast IT networks into a joint information environment is intended to enable and empower our military through a shared IT infrastructure consisting of federated networks with common configurations and management, a common set of enterprise services, within a common security architecture that creates a significantly more secure operating environment. With security a primary focus of JIE, DoD is accelerating the implementation of a set of activities that is creating a consolidate set of secure capabilities called the Joint Regional Security Stacks (JRSS) and modernizing the Department's core network transport capabilities. JRSS will be the foundational cornerstone to leverage a joint security construct protecting and defending DoD IT networks. The JRSS is a joint effort amongst the Military Services, led by DoD CIO, that when fully implemented will address the urgent need to enhance the defenses of the cyber warfighting domain; shrink attack surface from approximately1000 disparate ingress points to approximately50 ingress points; achieve a standard network security architecture; and accelerate achieving a standardized Command and Control platform for the JIE. Implementation of JIE is an evolutionary process that will become more complete and capable over time. Once these initial sets of foundational JIE elements are in place (i.e., JRSS and network modernization), fielding of the additional JIE operational capabilities will be enabled. Network modernization is itself a critical enabler to the JRSS effort. By increasing bandwidth and implementing Multi-Protocol Layer Switching (MPLS), the technical advantages will allow for separate Enterprise communities (i.e., Communities of Interest, logistics, medical, etc.) by enabling tailored cyber defense that is mission specific, not Service specific; significantly reducing the complexity and cost of long haul network transport across the Enterprise; and increasing bandwidth and more efficient utilization to support current and future Enterprise services.

The JIE will change the way we assemble, configure, and use new and legacy information technologies. It will consist of enterprise level network operations centers that will reduce the complexity and ambiguity of seeing and controlling the numerous networks within DoD; a set of core data centers - significantly reducing the current number of DoD

data centers while ensuring the information is secured and available where needed; and a standard security architecture that will reduce the number of organizationally owned firewalls, unique routing algorithms, and inefficient routing of information that currently exists today. Together with the single, authoritative identity management and access control, emerging cloud capability, mobile computing devices and data-focused applications, and common IT enterprise services, JIE will provide the information environment to flexibly create, store, disseminate, and access data, applications, and other computing services when and where needed. It will better protect the integrity of information from unauthorized access while increasing the ability to respond to security breaches across the system as a whole.

The ultimate beneficiary of JIE is the commander in the field, allowing for more innovative integration of information technologies, operations, and cyber security at a tempo more appropriate to today's fast-paced operational conditions. Specific benefits for mission effectiveness include:

- Rapid and dynamic response to support changing mission information needs under all operational scenarios;
- Timely and secure access to the data and services needed to accomplish assigned missions, regardless of location;
- Trusted connection from end to end with the assurance that activity will not be compromised; and
- Capabilities are still available during an event, even if they are degraded.

Specific benefits for increased security include:

- A consistent IT architecture to enable resiliency and defensibility;
- Shared situational awareness for network operators and defenders;
- Safe sharing with widest array of mission partners; and
- More freedom for mission commanders to take risk in the network.

Specific benefits for IT efficiencies include:

- Information assets are joint assets that can be leveraged for all Department missions;
- A consistent IT architecture supports effective fielding of Department capabilities; and
- Increased visibility about DoD IT expenditures through increased budget transparency.

The Department will have to make the required investments to effect the transition from the Department's as-is environment to the desired to-be state. The JIE will be operated and managed per the Unified Command Plan (UCP) using enforceable standards, specifications, and common tactics techniques & procedures (TTPs).

Leading the Department to Achieve an Information Advantage for the Warfighter and our Mission Partners

Information as a Strategic Asset

A robust information environment provides DoD and mission partners access to discoverable, authoritative, relevant, trusted, and actionable information and services to enable effective and agile decisions for mission success.

Major enabling objectives:

- Broaden Enterprise Services
- Increase Information Availability
- Build Community-based Solutions
- Leverage Cloud Computing Services
- Leverage Pilots and Experimentation
- Strengthen Information Sharing with Mission Partners

Interoperable Infrastructure

A more robust, reliable, rapidly scalable and interoperable infrastructure provides connectivity and computing capabilities that allow all DoD users and mission partners to access, share, and act on the information needed to accomplish their missions.

Major enabling objectives:

- Data Center Consolidation
- Shared Computing Resources
- Dynamic NetOps
- Increase Transmission Capability
- Enhanced Communications Interfaces
- Protect DoD Internet Equities

Synchronized and Responsive Ops

The DoD Information Enterprise (IE) infrastructure, critical assets, and capabilities are operated, secured, and defended in a synchronized manner by all DoD components to support commanders in achieving mission success.

Major enabling objectives:

- Manage NetOps Risk
- IE Situational Awareness and Management
- Aligned NetOps Policies and Standards

Cyberspace Operations

DoD can accomplish its missions in the face of cyber warfare by a capable adversary.

Major enabling objectives:

- Resilience to operate through cyber attacks
- Agile, safe information sharing with mission partners
- Robust attack detection diagnosis and response
- Information security

Optimizing IT Investments

An integrated information enterprise IT investment and IT portfolio management capability that maximizes the contribution of IT-IA investments to national security and Defense outcomes.

Agile IM/IT/IA Workforce

An agile IM/IT/IA workforce able to dynamically operate, defend, and advance the Defense Information Enterprise.

Exploit the Power of Trusted Information Sharing

Information is an asset: a source of power and a force multiplier. DoD and mission partners will obtain an information advantage when timely, secure and trusted information is available to all decision makers. We are moving rapidly to achieve a joint information environment where all data assets, services and information sharing solutions will be visible, accessible, understandable and trusted by all authorized users, except where limited by law, policy or security classifications. Independent data efforts across Combatant Commands, Military Departments (MILDEPS), Defense Agencies and Field Activities, and with mission partners will be aligned and leveraged to improve data quality, integration, transparency and sharing. Once achieved, warfighters will get the critical information they need to make timely decisions affecting operations.

The Department is committed to realizing the value of cloud computing by driving delivery and adoption of a secure, dependable DoD Enterprise Cloud Computing Environment that improves IT efficiencies, enhances mission effectiveness, meets mission needs and supports anywhere, anytime, information access, in alignment with Federal and Department-wide IT efficiency initiatives. The Department has specific challenges that pose careful adoption considerations, especially in areas of cyber security. DoD plays a key role in Federal Cloud Computing initiatives such as the Federal Risk and Authorization Management Program (FedRAMP) that is addressing security concerns. The DoD Cloud Computing Strategy provides an approach to move the Department to an end state that is an agile, secure, and cost effective service environment that can rapidly respond to changing mission needs. There are three key components of the Department's cloud strategy. The first component is the establishment of a private enterprise cloud infrastructure that supports the full range of DoD activities in unclassified and classified environments. The second is the establishment of an enterprise cloud access point that will enable commercial cloud services to securely connect to DoD networks in a provider agnostic manner. The third is to accelerate the Department's adoption of commercial cloud services by delegating decision making to the Component CIOs who have better understanding of the Mission Owner's requirements and ability to select providers that can also meet the Departments cybersecurity needs while providing capabilities that are at least as effective and efficient as those provided internally.

The Department will leverage the FedRAMP standardized security authorization process, including the accepted minimum security baseline for low and moderate services, and ongoing continuous monitoring for our less sensitive missions to ensure that appropriate security controls remain in place and are functioning properly. The Department has published additional security requirements (above the FedRAMP baselines) for our more sensitive missions.

Interoperable Infrastructure

Achieving mission success in today's operational environment, which increasingly involves joint, combined, and non-military partners, requires a dynamic and interoperable infrastructure consisting of communications, transport, and computing capabilities. Gaining and maintaining a persistent and dominant information advantage requires robust world-wide connectivity to enable highly effective information sharing across DoD and with its external mission partners. A reliable and rapidly scalable information infrastructure is the foundation for realizing enterprise alignment through greater integration of applications, services and systems, thereby strengthening operational effectiveness and efficiency. This effort focuses on delivering the integrated information enterprise infrastructure that DoD needs to harness the power of information.

The Department has identified opportunities to consolidate DoD IT infrastructure through several initiatives, one of which is Data Center Consolidation (DCC), consistent with the Federal Data Center Consolidation Initiative (FDCCI).

DoD Components are considering all options for achieving consolidation including infrastructure consolidation, virtualization and cloud computing, operational efficiencies, and

application rationalization to name a few. Based on Component plans to meet the DoD CIO directive to close 60% of datacenters by FY2018, the current DOD goal is close 849 data centers by the end of FY2016. DoD has confirmed the closure of 420 data centers since FY2011. DoD continues to identify additional datacenters for closure and is aggressively pursuing consolidation and virtualization. Based on the latest quarterly data center closure tracking, the DOD is on target to meet the FY2016 projected closure target by closing 233 data centers in FY2015 and 196 data centers in FY2016.

The savings estimates provided vary from previous estimates due to maturation of DoD's data center inventory and the cost model used to estimate savings. During FY2013, DoD's data center inventory changed as a result of additional discovery and reconciliation of invalid records. Further, inventory values for server counts, storage, operating systems, personnel, etc. were refined, and closure dates were adjusted to reflect current planning. To estimate the savings from the revised inventory, DoD used the most up to date version of DoD's cost model which is a derivative of OMB's data center Total Cost of Ownership (TCO) model. DoD's model provides a more realistic estimate of TCO and, therefore, more accurate estimates of realized and projected savings.

DOD Data Center Consolidation Savings Summary (FY11- FY16)

Summary Metrics (3)(5)	FY 2011	FY 2012	FY 2013	FY 2014	FY 2015 (2)	FY 2016 (2)
Fiscal Year Data Center Closures	59	80	111	170	233	196
Fiscal Year Impacted Servers from Closures (4)	3,821	4,346	3,812	2,126	6,014	7,142
Fiscal Year Savings (6)	$18,820,299	$5,346,648	$74,956,581	$24,061,591	$152,571,506	$271,903,480
Cumulative Year Savings	$18,820,299	$24,166,947	$99,123,528	$123,185,119	$275,756,626	$547,660,106

Notes:

(1) DOD Total Cost of Ownership Model Used (Version V1 Final) for Q4FY14 dataset

(2) Forward looking projections. Both efficiency and facility consolidation savings estimated for FY15 and FY16.

(3) In FY12 dollars

(4) Impacted Servers includes both decommissioned and moved servers.

(5) Investments required to implement efficiencies or close data centers are not captured within this analysis

(6) FY13 and FY14 savings increase from FY12 due to realized efficiency achievement

The Department recently compiled a global inventory of its data centers, and is establishing four classes of data centers to assist in the development and execution of our data center consolidation strategy. These four types of data centers are:

- Core Data Center (CDC) – delivers enterprise services and provides primary migration point for systems and applications; these are our most important data centers, strategically located to provide speed of access to global information requirements;

- Installation Processing Node (IPN) – provides local services to DoD installations and hosting systems not suited for CDCs, these will be located at the installation level, and will consolidate the duplicative data centers at the installations;

- Special Purpose Processing Node (SPPN) – provides compute and storage for fixed infrastructure or facilities, such as test ranges, labs, medical diagnostic equipment, and machine shops.

- Tactical/Mobile Processing Node (TPN) – provides support to the deployed warfighter at the tactical edge; these unique "data centers" directly support the warfighter in a disadvantaged or tactical environment, but connect back into the Generating Force information sources and core data centers.

Synchronized and Responsive Operations

Synchronized and responsive operations will enable all DoD components to operate, secure, and defend the Information Enterprise consistently. Operating in this coordinated manner will contribute significantly to mission success, help achieve and maintain cyberspace superiority within a contested environment, and support authorized users' access to timely and trusted information when and where it is needed. This effort entails establishing situational awareness from the core to the tactical edge, improving NetOps capabilities, enhancing C2 capabilities for allocating and managing IE resources, and strengthening enforcement of IE policies and standards. Information sharing across organizational boundaries and functional disciplines will be the norm. DoD personnel will increasingly rely upon timely access to trusted, secure information on a shared basis to facilitate decision-making processes at all levels of the command structure.

Cyberspace Operations

In recognition of cyberspace as an operational domain and the mission to defend the nation against cyber threats as directed by the President, this year's budget provides funds to increase defensive capabilities and develop the cyber Joint Force under a new force planning model.

The unique attributes of cyberspace operations require trained and ready cyberspace forces to detect, deter, and, if directed, respond to threats in cyberspace. Securing and defending cyberspace requires close collaboration among Federal, state and local governments, private sector partners, and allies and partners abroad. This year's budget establishes dedicated cyber teams to execute this mission on Defense Department networks and in support of Combatant Command and national missions.

This budget reflects an emphasis on enhancing our workforce to successfully execute defensive and offensive missions in cyberspace. The Department is implementing a new cyber force planning model that will realign military, civilian and contractor manpower positions (with associated support costs) under U.S. Cyber Command (USCYBERCOM) in a three-year phased build-up beginning in FY2014. This provides manpower, training and support costs for regional cyber mission teams to be located in Maryland, Texas, Georgia and Hawaii as well as other Combatant Command and military service locations. In addition, manpower at the National Security Agency continues to be funded to provide both cybersecurity and intelligence support to the USCYBERCOM teams. This overall force construct will provide capacity for the "Defend the Nation" mission, the cyber combat mission (in support of Combatant Command needs), and the cyberspace protection mission which defends Defense Department networks.

Oversight and Execution of DoD IT Investments

Optimizing IT investment is based on realizing the vision to institutionalize IT management best practices. Investment review boards that govern DoD IT investments across missions are central to this vision. These review boards are tasked to review the strategic relevance of all significant investments. Optimizing IT investments will be driven by wider adoption of IT investment governance, greater utilization of the DoD Enterprise Architecture, increased agility in acquisition processes, coordinated management of IT portfolios, improved oversight of compliance with applicable regulations, including Section 508 of the Rehabilitation Act for accessibility of IT to persons with disabilities, and the establishment of an environmentally responsible IT culture focused both on cost efficiencies and the reduction of the IT influenced carbon footprint.

Agile IT/Cyberspace Workforce

Timely, trusted and shared defense information is stored on and shared through transformative technology solutions that are designed, secured and implemented by a highly skilled workforce providing IT, Cybersecurity, and IT acquisition mission capabilities. Rapid technology advancements, coupled with increasing cyberspace challenges, require agile, fiscally responsible, and forward thinking individuals to architect, design, develop, acquire, operate, maintain and protect DoD IT/cyber resources, as well as strategic policy makers, planners and managers who oversee the governance of the DoD Information Enterprise. Strategic workforce planning supports the development of a broader balanced workforce with the experience, aptitude and creativity to deliver enterprise capabilities to support the business, intelligence and warfighting missions of the Department.

IT Investment Management

The Department's IT investment management strategy is based on leveraging Mission Area (warfighter, business, intelligence, and IT infrastructure), Component, and DoD level review boards and the Department's acquisition processes. The DoD CIO reviews and influences IT investments through its participation in the Department's overall governance processes. DoD manages IT investments in portfolios as part of the holistic management of broader organizational and functional portfolios to support the Department's mission success; ensure efficient and effective delivery of capabilities; and maximize return on investment to the Enterprise. In accordance with OMB guidance, DoD is reporting its IT/NSS budget in terms of a the following set of EA segments: Business Services, Enterprise Services, Core Mission (Warfighting), Core Mission (Intelligence).

IT plays a major role in each of these functions and services. The DoD CIO has a significant role in the decision processes, as well as serving as the lead for the IT infrastructure mission area. In December 2015 the department restructured its Defense Business Council to include CIO representation from the Military Departments and adding the DoD CIO as a co-chair of this body. The range of investments overseen by this body was expanded from just business systems to also include IT infrastructure and enterprise services. This enhancement in process will provide greater engagement by CIOs in business systems oversight and improve integration of business systems with enterprise infrastructure and services while driving down overall IT costs and reducing the number of duplicative systems.

eGovernment

The Department of Defense has and continues to benefit from the implementation of IT Management requirements supporting the President's agenda for transparency, information sharing, alignment of architectures, advancement of new technologies, and Federal-wide initiatives. E-Government Projects/Initiatives support the implementation

and oversight, within the Department, of Federal-wide IT initiatives such as Enterprise Architecture, Federal Information Sharing, Cloud Computing, E-Government Analysis & IT Portfolio Management, IT Consolidation, and IM/IT/IA workforce development. The following initiatives will be funded by DoD agency contributions[1] in FY2016.

Initiative	FY15	FY16
Financial Management LoB	$178,140	$187,342
Human Resources Management LoB	$260,870	$260,870
Federal Health Architecture LoB	$2,094,000	$2,356,000
Geospatial LoB	$42,000	$225,000
Budget Formulation and Execution LoB	$105,000	$105,000
Grants.gov	$666,561	$584,477
Performance Management LoB		$43,000
DoD Total	**$3,346,571**	**$3,718,689**

Table 1(Funding identified in actual dollars)

Objective of eGovernment Initiatives:

Financial Management LoB / Managing Partner, General Services Administration - FM LoB's vision is to create government-wide financial management solutions that are efficient and improve business performance while ensuring integrity in accountability, financial controls, and mission effectiveness. FM LoB is working in coordination with the Chief Financial Officer's Council (CFOC), the COFAR, and partner agencies to bring together the financial management and financial assistance communities to achieve this vision, improve transparency of federal spending, and streamline agency operations. A benefit for most agencies will be a new synergy and coordination of top-down policy and guidance across these domains, allowing agencies to streamline operations in more standardized manner.

Human Resources LoB / Managing Partner, Office of Personnel Management – The DOD is one of the approved service providers for the HR LoB. Core HR services are provided by DOD for its Military Services, Defense Agencies and civilian customer agencies through the Defense Civilian Personnel Advisory Service (DCPAS) and the Defense Finance and Accounting Service (DFAS). This initiative allows the DOD to optimize the cost of managing HR systems and processes across a worldwide customer base and to reduce costs of performing these functions individually. Involvement in the HR LoB permits the DOD to benefit from best practices and government-wide strategic HR

[1] Agency contributions reflect commitments of funding and/or in-kind services provided by partner agencies to initiative managing partner agencies in support of developing, implementing, and/or migrating to E-Government common solutions. Contribution amounts are determined annually through collaborative, inter-agency E-Government initiative governance structures and are subject to approval by OMB.

management. Participation in the HR LoB presents opportunities to partner with other providers in obtaining core functional changes for jointly used commercial HRIT products. This approach contributes to DOD's goal for implementation of efficient, state-of-the-art, and cost-effective enterprise HR solutions.

Federal Health Architecture LoB / Managing Partner, Department of Health and Human Services - Federal Health Architecture (FHA) coordinates government-wide solutions for interoperable and secure health information exchange that address agency business priorities, while protecting citizen privacy. In addition to the DOD, FHA serves the needs of more than twenty Federal agencies in domains as diverse as veterans' healthcare, public health monitoring, long-term care and disability services, research, and tribal health services.

Geospatial LoB / Managing Partner, Department of the Interior – DOD benefited from improved access to geospatial information that led to improved productivity, improved mission delivery, and increased service to citizens. Geospatially enabling traditional business data improved business process efficiency, allowed for geographically based work planning and investment processes, assisted in infrastructure asset tracking, improved mission delivery, and promoted the use of business intelligence in the Department's decision support systems.

Budget Formulation and Execution LoB / Managing Partner, Department of Education - The BFE LoB provides agencies with technological solutions, tools, and services for enhancing budgeting, analysis, document production, and data collection. The BFE LoB also provides tools for secure collaboration and online meetings, and human capital solutions. Through the BFE LoB, agencies can share best practices for budgeting activities, identify training and educational opportunities, and communicate core competencies and career path options for budget analysts. Finally, the BFE LoB provides governance solutions, providing year-round coordination via a program management office, furthering the idea of sharing and re-use, and setting standards for data and data exchange.

Grants.gov - Grants.gov provides a single website to find and apply for federal discretionary grants. Grants.gov provides over one million organizations a single web site where they can find and apply for over $153 billion worth of grants distributed annually. Grants.gov empowers smaller agencies with limited resources to improve the reach of their grant programs, and provides larger agencies with the benefit of process standardization, cost savings, and increased visibility. The program is funded by the 26 Federal grant-making agencies, each providing support commensurate with its size according to a formula approved by the Council on Financial Assistance Reform (COFAR).

Notes:

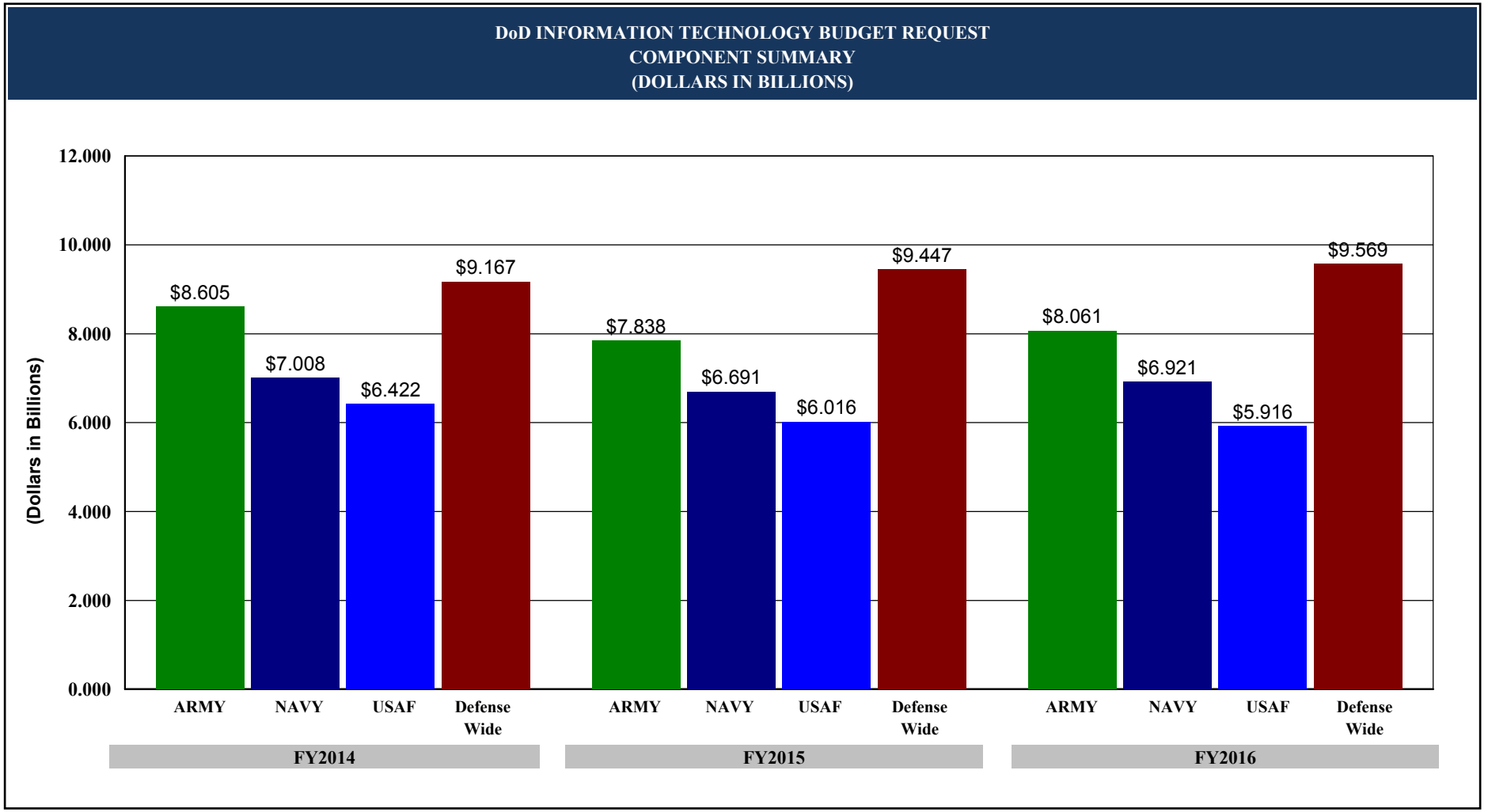
FY2014 through FY2016 each contain Base and Overseas Contingency Operations (OCO) funding amounts. FY2016 contains Base and a small amount ($240.5M) of estimated OCO funding, but does not include the final FY2016 OCO request. FY2017 through FY2020 are Base funding only.

The FY2016 Department of Defense IT Budget materials are available on the web at: https://snap.cape.osd.mil/snapit/BudgetDocs2016.aspx

Page left intentionally blank

DoD INFORMATION TECHNOLOGY BUDGET REQUEST BY DEPARTMENT (DOLLARS IN MILLIONS)			
DEPARTMENT	**FY2014**	**FY2015**	**FY2016**
DEPARTMENT OF ARMY	$8,605.265	$7,838.124	$8,061.001
DEPARTMENT OF NAVY	$7,007.599	$6,690.821	$6,921.037
DEPARTMENT OF AIR FORCE	$6,421.626	$6,015.825	$5,916.364
DEFENSE WIDE ACTIVITIES	$9,167.260	$9,447.281	$9,568.934
DOD TOTALS	**$31,201.750**	**$29,992.051**	**$30,467.336**

Page left intentionally blank


DoD INFORMATION TECHNOLOGY BUDGET REQUEST
COMPONENT SUMMARY
(DOLLARS IN BILLIONS)
(Dollars in Billions)
12.000
10.000
8.000
6.000
4.000
2.000
0.000
$8.605
$7.008
$6.422
$9.167
$7.838
$6.691
$6.016
$9.447
$8.061
$6.921
$5.916
$9.569
ARMY
NAVY
USAF
Defense Wide
FY2014
FY2015
FY2016

Page left intentionally blank

DoD INFORMATION TECHNOLOGY BUDGET REQUEST BY COMPONENT (DOLLARS IN MILLIONS)			
	FY2014	FY2015	FY2016
GRAND TOTAL	**$31,201.750**	**$29,992.051**	**$30,467.336**
DEPARTMENTS	**$22,034.490**	**$20,544.770**	**$20,898.402**
ARMY	$8,605.265	$7,838.124	$8,061.001
NAVY	$7,007.599	$6,690.821	$6,921.037
USAF	$6,421.626	$6,015.825	$5,916.364
DEFENSE AGENCIES	**$8,319.740**	**$8,630.355**	**$8,756.158**
DARPA	$34.427	$35.119	$35.645
DCAA	$37.511	$30.633	$31.633
DCMA	$132.155	$136.057	$133.170
DeCA	$70.881	$115.167	$140.597
DFAS	$373.794	$397.725	$362.304
DHA	$1,945.969	$2,001.282	$2,396.459
DISA	$3,079.395	$3,189.612	$3,008.301
DLA	$1,208.077	$1,235.448	$1,184.163
DPAA	$3.003	$8.327	$8.542
DSCA	$17.614	$12.807	$11.453
DSS	$33.638	$36.060	$40.095
DTRA	$126.123	$98.451	$103.718
JCS	$98.773	$87.666	$110.164
MDA	$199.506	$247.346	$241.811
OSD	$76.534	$115.439	$75.647
OSD/CAPE	$14.102	$16.970	$17.109
PFPA	$22.048	$34.999	$35.314
SOCOM	$345.534	$244.115	$286.963
TRANSCOM	$420.247	$494.026	$444.564
USD(AT&L)	$80.409	$93.106	$88.506

BY COMPONENT - continued (DOLLARS IN MILLIONS)			
	FY2014	FY2015	FY2016
FIELD ACTIVITIES	**$847.520**	**$816.926**	**$812.776**
DCMO	$10.211	$4.833	$2.223
DHRA	$337.324	$299.253	$292.858
DMACT	$71.411	$69.511	$68.613
DODEA	$89.760	$91.320	$93.468
DTIC	$23.741	$19.416	$20.898
DTSA	$4.726	$4.743	$4.861
IG	$32.136	$42.881	$39.376
NDU	$9.183	$9.183	$10.009
WHS	$269.028	$275.786	$280.470

DoD INFORMATION TECHNOLOGY BUDGET REQUEST
BY SEGMENT
(DOLLARS IN MILLIONS)

SEGMENT	FY2014	FY2015	FY2016
ACQUISITION	$488.567	$507.987	$481.100
BATTLESPACE AWARENESS-ENVIRONMENT	$361.104	$379.221	$461.227
BATTLESPACE AWARENESS-ISR	$98.475	$82.408	$68.663
BATTLESPACE NETWORKS	$3,065.072	$2,636.675	$2,882.670
BUILDING PARTNERSHIPS	$82.364	$82.764	$93.352
BUSINESS SERVICES TBD	$159.668	$134.641	$121.631
COMMAND & CONTROL	$2,438.495	$2,767.223	$2,620.544
CORE MISSION TBD	$140.503	$139.979	$159.902
DOD IT INFRASTRUCTURE	$16,071.671	$14,728.522	$14,449.990
FINANCIAL MANAGEMENT	$772.352	$821.577	$792.331
FORCE APPLICATION	$588.447	$499.559	$534.739
FORCE MANAGEMENT	$105.387	$98.458	$94.796
FORCE TRAINING	$287.926	$176.998	$245.105
HEALTH	$963.266	$1,041.426	$1,389.434
HUMAN RESOURCE MANAGEMENT	$1,685.830	$1,835.771	$1,911.925
INSTALLATION SUPPORT	$288.307	$280.646	$276.779
IT MANAGEMENT	$800.900	$854.824	$950.778
LOGISTICS/SUPPLY CHAIN MANAGEMENT	$2,557.421	$2,712.490	$2,682.889
PROTECTION	$245.995	$210.882	$249.481
DOD TOTALS	**31,201.750**	**29,992.051**	**30,467.336**

Page left intentionally blank

DoD INFORMATION TECHNOLOGY BUDGET REQUEST SEGMENTS BY COMPONENT (DOLLARS IN MILLIONS)			
ACQUISITION	**FY2014**	**FY2015**	**FY2016**
ARMY	$96.166	$93.347	$78.715
NAVY	$179.206	$204.670	$207.189
AIR FORCE	$63.577	$78.795	$75.864
DEFENSE WIDE	$149.618	$131.175	$119.332
	$488.567	$507.987	$481.100
BATTLESPACE AWARENESS-ENVIRONMENT	**FY2014**	**FY2015**	**FY2016**
ARMY	$210.451	$240.411	$305.273
NAVY	$78.086	$67.711	$77.462
AIR FORCE	$72.567	$71.099	$78.492
	$361.104	$379.221	$461.227
BATTLESPACE AWARENESS-ISR	**FY2014**	**FY2015**	**FY2016**
ARMY	$1.060	$1.090	$0.000
NAVY	$82.955	$59.522	$49.999
AIR FORCE	$14.460	$21.796	$18.664
	$98.475	$82.408	$68.663
BATTLESPACE NETWORKS	**FY2014**	**FY2015**	**FY2016**
ARMY	$1,227.235	$1,073.959	$1,154.608
NAVY	$642.003	$587.493	$575.672
AIR FORCE	$598.611	$488.136	$589.826
DEFENSE WIDE	$597.223	$487.087	$562.564
	$3,065.072	$2,636.675	$2,882.670
BUILDING PARTNERSHIPS	**FY2014**	**FY2015**	**FY2016**
AIR FORCE	$63.944	$68.169	$80.066
DEFENSE WIDE	$18.420	$14.595	$13.286
	$82.364	$82.764	$93.352

SEGMENTS BY COMPONENT - continued (DOLLARS IN MILLIONS)			
BUSINESS SERVICES TBD	**FY2014**	**FY2015**	**FY2016**
ARMY	$0.000	$1.856	$1.904
NAVY	$128.007	$109.925	$90.069
AIR FORCE	$7.747	$6.241	$6.401
DEFENSE WIDE	$23.914	$16.619	$23.257
	$159.668	$134.641	$121.631
COMMAND & CONTROL	**FY2014**	**FY2015**	**FY2016**
ARMY	$229.592	$356.809	$387.758
NAVY	$454.179	$498.085	$430.572
AIR FORCE	$1,277.756	$1,446.048	$1,338.481
DEFENSE WIDE	$476.968	$466.281	$463.733
	$2,438.495	$2,767.223	$2,620.544
CORE MISSION TBD	**FY2014**	**FY2015**	**FY2016**
ARMY	$10.827	$3.367	$13.240
NAVY	$43.782	$57.890	$70.317
AIR FORCE	$83.480	$75.148	$72.755
DEFENSE WIDE	$2.414	$3.574	$3.590
	$140.503	$139.979	$159.902
DOD IT INFRASTRUCTURE	**FY2014**	**FY2015**	**FY2016**
ARMY	$4,556.395	$3,911.962	$3,873.149
NAVY	$3,723.070	$3,399.300	$3,503.508
AIR FORCE	$3,006.356	$2,405.105	$2,283.531
DEFENSE WIDE	$4,785.850	$5,012.155	$4,789.802
	$16,071.671	$14,728.522	$14,449.990
FINANCIAL MANAGEMENT	**FY2014**	**FY2015**	**FY2016**
ARMY	$126.332	$118.207	$110.633
NAVY	$96.645	$108.424	$105.926
AIR FORCE	$154.619	$161.928	$213.651
DEFENSE WIDE	$394.756	$433.018	$362.121
	$772.352	$821.577	$792.331

SEGMENTS BY COMPONENT - continued (DOLLARS IN MILLIONS)			
FORCE APPLICATION	**FY2014**	**FY2015**	**FY2016**
ARMY	$210.870	$199.888	$167.715
NAVY	$122.417	$59.183	$103.358
AIR FORCE	$211.516	$206.585	$228.246
DEFENSE WIDE	$43.644	$33.903	$35.420
	$588.447	$499.559	$534.739
FORCE MANAGEMENT	**FY2014**	**FY2015**	**FY2016**
ARMY	$29.957	$17.116	$9.457
NAVY	$25.278	$31.611	$38.753
AIR FORCE	$41.971	$40.790	$35.884
DEFENSE WIDE	$8.181	$8.941	$10.702
	$105.387	$98.458	$94.796
FORCE TRAINING	**FY2014**	**FY2015**	**FY2016**
ARMY	$238.769	$127.437	$174.459
NAVY	$15.174	$12.869	$13.032
AIR FORCE	$26.000	$28.491	$44.004
DEFENSE WIDE	$7.983	$8.201	$13.610
	$287.926	$176.998	$245.105
HEALTH	**FY2014**	**FY2015**	**FY2016**
NAVY	$3.497	$4.874	$5.041
DEFENSE WIDE	$959.769	$1,036.552	$1,384.393
	$963.266	$1,041.426	$1,389.434
HUMAN RESOURCE MANAGEMENT	**FY2014**	**FY2015**	**FY2016**
ARMY	$575.701	$702.797	$769.094
NAVY	$403.822	$409.084	$413.956
AIR FORCE	$166.249	$208.153	$223.768
DEFENSE WIDE	$540.058	$515.737	$505.107
	$1,685.830	$1,835.771	$1,911.925

SEGMENTS BY COMPONENT - continued (DOLLARS IN MILLIONS)			
INSTALLATION SUPPORT	**FY2014**	**FY2015**	**FY2016**
ARMY	$126.502	$132.466	$131.404
NAVY	$58.597	$57.267	$57.312
AIR FORCE	$91.280	$80.996	$80.110
DEFENSE WIDE	$11.928	$9.917	$7.953
	$288.307	$280.646	$276.779
IT MANAGEMENT	**FY2014**	**FY2015**	**FY2016**
ARMY	$36.502	$34.169	$32.145
NAVY	$254.666	$288.817	$383.263
AIR FORCE	$58.513	$56.826	$57.538
DEFENSE WIDE	$451.219	$475.012	$477.832
	$800.900	$854.824	$950.778
LOGISTICS/SUPPLY CHAIN MANAGEMENT	**FY2014**	**FY2015**	**FY2016**
ARMY	$821.629	$749.996	$758.964
NAVY	$677.200	$718.692	$765.535
AIR FORCE	$421.110	$499.532	$413.916
DEFENSE WIDE	$637.482	$744.270	$744.474
	$2,557.421	$2,712.490	$2,682.889
PROTECTION	**FY2014**	**FY2015**	**FY2016**
ARMY	$107.277	$73.247	$92.483
NAVY	$19.015	$15.404	$30.073
AIR FORCE	$61.870	$71.987	$75.167
DEFENSE WIDE	$57.833	$50.244	$51.758
	$245.995	$210.882	$249.481
DoD Totals	**$31,201.750**	**$29,992.051**	**$30,467.336**

DoD INFORMATION TECHNOLOGY BUDGET REQUEST BY MISSION AREA (DOLLARS IN MILLIONS)			
MISSION AREA	**FY2014**	**FY2015**	**FY2016**
BUSINESS	$6,915.411	$7,334.538	$7,656.089
DEFENSE INTELLIGENCE	$98.475	$82.408	$68.663
ENTERPRISE INFORMATION ENVIRONMENT	$16,872.571	$15,583.346	$15,400.768
WARFIGHTING	$7,315.293	$6,991.759	$7,341.816
DOD TOTALS	**$31,201.750**	**$29,992.051**	**$30,467.336**

Page left intentionally blank